PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : B60R 25/04	A1	(11) International Publication Number: WO 98/16411 (43) International Publication Date: 23 April 1998 (23.04.98)

(21) International Application Number: PCT/GB96/02517

(22) International Filing Date: 14 October 1996 (14.10.96)

(71) Applicant (*for all designated States except IS US*): NYLOTECHNICS (PROPRIETARY) LIMITED [ZA/ZA]; 16 Bellamont Road, Umdloti Beach, Kwazulu-Natal 4350 (ZA).

(71) Applicant (*for IS only*): DYER, Alison, Margaret [GB/ZA]; 10 Veldtuin Place, Morningside, Sandton 2057 (ZA).

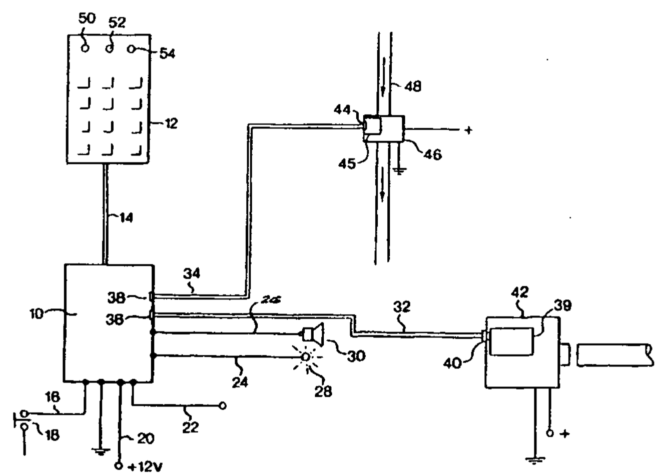
(72) Inventor; and
(75) Inventor/Applicant (*for US only*): ROBJANT, Graham, Edgar [ZA/ZA]; 159 Nicolson Road, Glenwood, Durban 4001 (ZA).

(74) Agents: KILLIN, Stephen, James et al.; Venner, Shipley & Co., 20 Little Britain, London EC1A 7DH (GB).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: VEHICLE SECURITY SYSTEM



(57) Abstract

A vehicle security system comprises a main control circuit (10) and first and second enabling/disabling circuits (39, 45) linked to the control circuit by means of first and second fibre optic cables (31, 34). The enabling/disabling circuits may be arranged to control a solenoid-operated fuel valve (46) and a starter motor (42) of the vehicle. First and second coded infrared signals are transmitted from the control circuit to the enabling/disabling circuits, and the enabling/disabling circuits are maintained in an enabled mode only on continuous receipt of the coded infrared signals, with the break in transmission of the signals causing the enabling/disabling circuits to become disabled. A remote keypad (12) is provided for generating a coded enabling signal for receipt at the control circuit, which in turn generates the first and second coded enabling signals. Door and ignition sensors (18, 22) are provided for sensing the turning on of the vehicle or the opening of the vehicle door, and logic circuitry is arranged to selectively arm, disarm or immobilise the vehicle, depending on the condition of the vehicle door and ignition sensors, with the armed vehicle being arranged to become immobilised on receipt (60) of a remote disabling signal.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

VEHICLE SECURITY SYSTEM

BACKGROUND TO THE INVENTION

This invention relates to a security system, and in particular to a vehicle security system for protecting a vehicle.

Certain types of existing vehicle immobilising systems have a central control circuit and a remote immobilising circuit which are linked to one another either via electrical wiring incorporated in the harness of the vehicle or via separate dedicated electrical wiring. A disadvantage of a hard wired system of this type is that once the relevant wire has been located, it can easily be bridged or bypassed. Such a wire is typically linked to a fuel solenoid or the like which is typically responsive to a non-characteristic and easily generated high voltage signal.

SUMMARY OF THE INVENTION

According to the invention there is provided a vehicle security system comprising a control circuit, a first enabling/disabling circuit remote from the control circuit and being arranged to immobilise the vehicle, a first optical link extending between the control circuit and the first enabling/disabling circuit, and enabling means for enabling the enabling/disabling circuit via the first optical link, the enabling means including enabling signal generating means for generating a first characteristic enabling signal for continuous transmission via the first optical link, whereby the enabling/disabling circuit is arranged to immobilise the vehicle on non-receipt of the first characteristic enabling signal.

Preferably, the enabling means includes coded entry means for generating a second coded enabling signal, the enabling signal generating means being responsive to the second coded enabling signal.

In one form of the invention, the security system comprises first sensing means for sensing an act of entry into or exit from the vehicle, the control circuit including first arming means responsive to the first sensing means for preventing the enabling signal generating means from responding to the second coded enabling signal.

In an alternative form of the invention, the security system comprises first sensing means for sensing an act of entry into exit from the vehicle, the control circuit including first arming means responsive to the first sensing means for arming the enabling/disabling circuit via the control circuit such that the vehicle is in an armed mode in which it is able to respond to a

remote disabling signal, but can still be driven.

Conveniently, the invention includes second sensing means for sensing the activating of the vehicle, the first arming means also being responsive to the second sensing means.

The first sensing means may be arranged to sense the opening of a door of the vehicle, and the second sensing means may be arranged to sense the turning on of the vehicle ignition switch.

Typically, the enabling signal generating means includes modulating circuitry for generating a characteristic modulated or coded optical signal as an enabling signal, and the first enabling/disabling circuit includes detection circuitry arranged to respond only to the characteristic modulated or coded signal.

Advantageously, the vehicle security system includes a second enabling/disabling circuit remote from the control circuit and being arranged to immobilise the vehicle, and a second optical link extending between the control circuit and the second enabling/disabling circuit.

The first and second optical links may include first and second fibre optic cables, first and second optical transmitters and first and second optical receivers.

In one form of the invention, the control circuit includes logic means for enabling the enabling signal generating means only in the event of the first arming means not having responded to both the first and second sensing

means.

The logic means may further include timing means for timing a delay between receipt of an arming signal from the first sensing means and the receipt of an arming signal from the second sensing means, the logic means being arranged to immobilise the vehicle in the event of the delay exceeding a predetermined time period.

The timing means may be arranged to time a delay between non-receipt of an arming signal from the second sensing means and receipt of an arming signal from the first sensing means, the logic means being arranged to immobilise the vehicle in the event of the delay exceeding a predetermined time period.

In one form of the invention, the vehicle security system includes a receiver for receiving the remote disabling signal from a remote transmitter unit, the first arming means including a primary immobilising circuit arranged to immobilise the vehicle on receipt of the disabling signal, the primary immobilising circuit being responsive to the disabling signal to immobilise the vehicle only in the event of the primary immobilising circuit being armed via the first arming means.

The vehicle security system may incorporate second sensing means for sensing the activating of the vehicle, the first arming means being responsive to the first and second sensing means, and the control means being arranged to arm the primary immobilising circuit for receipt of a remote disabling signal in the event of the first arming means having responded to the first and second sensing means.

The first and second enabling/disabling circuits may be arranged to selectively disable the vehicle by cutting off the fuel supply via a solenoid-operated fuel valve, to disable the vehicle ignition system, disable a starter motor, or disable an automatic transmission system.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a highly schematic block diagram of a first embodiment of a vehicle security system of the invention;

Figure 2 shows a highly schematic block diagram of a second embodiment of the vehicle security system of the invention;

Figure 3 shows a circuit diagram of an analogue circuit of the main components of the security system of Figure 2;

Figures 4A to 4D show a detailed circuit diagram of a third embodiment of the vehicle security system of the invention incorporating a microprocessor-based circuit;

Figure 5 shows a flowchart illustrating the basic operation of the security system of Figures 4A to 4D;

Figures 6A & 6B show detailed circuit diagrams of a fourth embodiment of the vehicle security system of the

invention; and

Figure 7 shows a flowchart illustrating a basic operation of the vehicle security system of Figures 6A and 6B.

DESCRIPTION OF THE EMBODIMENTS

The vehicle security system illustrated in Figure 1 has at its heart a central control unit 10 arranged to receive a digital signal from a keypad unit 12 via a connecting cable 14. Further input lines connected to the control unit 10 include a door switch input line 16 connected to a door switch 18 of the driver's door, a power line 20 connected to the vehicle battery, and an ignition-on line 22 connected to the ignition switch of the vehicle. Output lines 24 and 26 are connected to the respective hazard lights 28 and a siren 30 of the vehicle. All of the above lines comprise conventional electrical wiring which may or may not be incorporated in the vehicle wiring harness.

Additional outputs from the control unit include first and second fibre optic links comprising cables 32 and 34 which are coupled to respective infrared LED or other pulse coded light source transmitters 36 and 38 at the control unit. The fibre optic cable 32 terminates at a first remote immobilising circuit 39 including a photo-transistor receiver 40 which is in turn linked to disabling/enabling circuitry which is enclosed within an encapsulated or potted solenoid and starter motor housing 42. Similarly, the fibre optic cable 34 terminates at a photo-transistor receiver LED 44 which is in turn linked to a second remote immobilising circuit 45 encapsulated within a fuel solenoid or pump 46 which is arranged to control the flow of fuel along a

fuel line 48.

The keypad 12 has various indicator LED's, including a transmitter pulse LED 50, an entry code LED 52 and an immobiliser LED 54, and is located on or next to the vehicle dashboard within reach of the driver. Prior to the PIN code being entered on the keypad, the driver's door of the vehicle has to be closed and the ignition of the vehicle needs to be turned on. The control unit 10 senses these conditions via the door-switch line 16 and the ignition-on line 22. The driver then enters a five digit code a relatively short predetermined time after the door has been closed and the ignition has been turned on. Once the correct code has been entered, the control unit receives the code and causes associated encoded optical signals to be transmitted via the respective infrared transmitters 36 and 38 along their respective fibre optic cables 32 and 34 to the respective opto-receivers 40 and 44. On receipt of the correct encoded optical signals, the immobilizing circuits 39 and 45 are enabled for enabling the respective starter motor 42 and fuel solenoid or pump 46. The first and second immobilizing circuits 39 and 45 are configured in such a way that they require a continuous receipt of the encoded optical signals in order to stay in the enabled mode. This means that they will immediately default to the disabled mode as soon as they are no longer receiving the coded optical signals for whatever reason, such as disconnection of the vehicle battery, cutting of one of the fibre optic cables 32 to 34 or any other discontinuity arising in the fibre optic cables caused by an attempt to bypass or broach the cables.

Referring now to Figure 2, a schematic view of an extended version of the vehicle security system is shown. Those components of the security system which are identical to the components illustrated in Figure 1 are identified

with the same numerals. The control unit 10 includes an arming circuit 56 and a primary immobiliser circuit 58 from which the fibre optic cables 32 and 34 extend. The arming circuit 56 is arranged to receive inputs from a receiver 60, as well as the keypad 12 and the ignition and door switch input lines 22 and 16. The receiver 60 is in turn coupled to a trip/reset unit 62. The RF receiver 60 is arranged to receive disabling signals from a remote immobilizing unit in the form of a remote transmitter unit 64, which may be solar-powered, and which includes a battery recharger 66, a pulsing unit 68 and a 440 MHz transmitter 69. The transmitter unit 64 may be located at various checkpoints or entry-exit points such as toll stations, border posts, parking lot exists and the like. Transmitters may be also fitted into roving vehicles such as police or security vehicles. The range of the transmitters may vary between 30 meters and 100 meters, with all the transmitters being on the same frequency.

If the allocated PIN code is not entered via the disarming keypad 12, it may still be possible to drive the vehicle under certain conditions. However, as soon as the vehicle approaches an immobilizing transmitter 64 at a security check point at a toll station or the like, the signal from the transmitter is received by the receiver, which in turn relays a signal to the arming circuit 56. The arming circuit 56 activates the immobiliser circuit 58, which in turn cuts power to the ignition system via an ignition line 70, only once a solenoid 71 has been activated via the brake pedal of a vehicle. In this way the vehicle can only be immobilized once the vehicle brakes have been applied, which prevents potentially hazardous situations in which the vehicle may cut out when accelerating for overtaking or the like. The hazard lights 28 and horn are simultaneously activated via the respective output lines 24 and 26. Once the vehicle is immobilized, it will then be necessary for the

driver to produce some form of identification and to enter the vehicle's PIN code. If it is not possible for the driver to re-start the vehicle and to produce adequate identification, he or she will then be apprehended on suspicion of vehicle theft.

If the driver is hijacked at a stop street, typically when the vehicle is running and the code has been entered correctly, opening of the driver's door is sensed via the door switch line 16 at the arming circuit 56. The secret PIN code is then cancelled, enabling or arming the final stage of the receiver unit so that it is receptive to signals from the transmitter 64. As soon as the vehicle passes a security checkpoint, disabling signals from the transmitter 64 will immobilise the vehicle immediately, as a result of which the vehicle can be recovered and the hijacker can be apprehended at a location where there are sufficient security personnel. In most situations, the driver will have been thrown out of the vehicle at the location where it was hijacked. An advantage of the security system of the type described is that the vehicle is not immediately immobilised on being hijacked, but is only immobilised when the vehicle is far away from the driver, who will then be a safe distance from the hijackers. In the event of the driver being kidnapped, in the particular embodiment described above, the immobilisation of the vehicle at a security checkpoint or the like ensures that the available security personnel can apprehend the hijackers and protect the kidnapped driver.

A further feature of the security system of the invention permits monitoring of a vehicle fitted with the security system. When the vehicle is left unattended and parked, a roving security unit fitted with a transmitter unit 64 will actively immobilize the vehicle and the transmitter pulse LED 50 will flash, indicating that the roving security unit is performing its duty. The

LED will reset once the ignition key has been turned on, the doors are closed, and the correct PIN code has been entered.

In Figure 3, a more detailed circuit diagram of the control circuitry is shown. The enabling keypad 12 is linked to keypad control circuitry 72. As an option, a remote keypad or coded transmitter unit 73 may be provided in place of the keypad 12, with a second receiver unit 76 being arranged to receive signals from the coded transmitter unit 73 which are relayed to the keypad control circuitry 72. After the correct PIN code has been entered, an output control line 78 receives a positive signal from the keypad control circuitry 72 which travels via diodes D1 and D2 to the bases of respective transistors TR1 and TR2. The transistor TR2 generates a negative-going signal which activates a 555 timer IC 80, causing the timer IC 80 to time out for approximately 3 seconds, after which it generates an output signal which turns on the transistor TR3 and activates a bleeper 82 and an LED D3 before resetting.

On receiving the positive output along the output control line 78, the transistor TR1 generates a negative pulse which is fed to a NOT gate 84 forming part of logic circuitry 86 which is configured as a comparator to compare signals from the receiver 60 and the keypad control circuitry 72. The logic circuitry 86 is biased in such a way that a signal along the output control line 78 holds an output line 88 leading to the base of a transistor TR4 at zero. The transistor TR4 in turn controls the operation of a transistor TR5, which maintains the immobiliser relay RL1 in the de-energised state for as long as the transistors TR4 and TR5 are off. With the door switch 18 closed, the negative voltage normally present when the door is open is removed from the input of a NOT gate 90 forming part of the logic circuitry

86, with the result that the logic circuitry has a zero output at the NOT gate.

If the vehicle passes a remote transmitter post in the condition described above, the receiver 60 will pick up a signal from the remote transmitter 64 (see Figure 2) and will output a signal to the input of the NOT gate 90 via diode D4 and the input of the timer IC 80 via diode D5. The timer IC 80 will thus be activated, causing the buzzer and LED 82 and D3 to beep and flash, indicating that a transmitter has been passed. Owing to the negative bias from the keypad circuitry 72, the input signal from the transmitter will have no effect on the output of the logic circuitry 86. If the code has not been entered prior to driving the vehicle, the door was subsequently opened or the code was cleared by a switch mounted on the floor panel of the vehicle, the vehicle will be immobilized on passing a transmitter in the following manner.

The output of the logic circuitry on the output line 88 is held low by virtue of the signal from the keypad circuitry 72, with the result that once the code is cleared, the output from the logic circuitry is no longer controlled via the keypad. The NOT gate 90 will consequently be in a position to switch the output from the logic circuitry to a logic "1" once the signal has been picked up from the transmitter via the receiver 60. This will be effective in turning on transistor TR4, which in turn will allow immobilizing relay RL1 to be energised via transistor TR5. Energising of the relay RL1 will cause the normally closed contacts 92 and 94 to open. The opposite terminals of the contacts 92 are linked to an ignition relay RL3, which will subsequently be de-energized so as to immobilize the vehicle.

The infrared transmitter unit 38 is linked across the immobilizing relay RL1,

with the result that energising of the coil will cause the fuel solenoid 46 to block the fuel line in the manner described further on in the specification.

Delay circuitry 98 incorporating a timing capacitor C1 is coupled to an input branch line 100 extending from an output of the NOT gate 84, and is in turn arranged to energize a relay RL4 via a transistor TR6 only once the capacitor C1 is fully charged. The relay RL4 is in turn arranged to a close pair of contacts 102 and 104 which lead to the respective hazard lights 28 and horn 30 of the vehicle. The horn and hazard lights are activated for a period of about 30 seconds, after which the capacitor C1 discharges completely.

The infrared transmitter unit 38 is shown coupled to the encapsulated fuel solenoid 46 via the optical line 34. The transmitter unit 38 is in turn enabled by the voltage across relay coil RL1. The transmitter unit 38 has at its heart a 555 timer IC 102 which has an output 104 coupled to the base of a transistor 106 which acts as a switch for turning an infra-red LED 108 on and off at a specific modulating frequency determined by the timer 1C 102. The infra-red LED 108 transmits a signal via the optical cable 34 to an infra-red receiver 110. The receiver 110 is in turn arranged to control the operation of immobilizing circuitry 112, which also includes a 555 timer IC 114 which is tuned to exactly the same modulating frequency as the timer IC 102. Consequently, the timer IC 114 will only deliver an output signal along its output line 116 in the event of exact frequency and signal matching occurring between the transmitter unit 108 and the receiver 110. The output 116 is in turn arranged to drive a transistor 118 which activates a solenoid 120 so as to open a solenoid valve 122 which extends into and blocks a fuel line 48 only for as long as a valid coded optical disarming signal is

continuously received at the transistor 118. Any break in transmission of this characteristic signal will lead to immediate closure of the valve.

Referring now to Figures 4A to 4D, detailed circuit diagrams of the various components making up a third largely software-based embodiment of a vehicle security system are illustrated. In Figure 4A, a main CPU 140 processes the programme stored in the EPROM section of a memory chip 142, which also contains address decoder circuitry and RAM memory. Both the CPU 140 and its associated memory 142 are linked to a universal asynchronous receiver/transmitter (UART) 144. The UART is connected either to a PC connector 144A via a selector circuit 145 or to an RF receiver connector 144B via the selector circuit 145 and a level translator 144C. Pin 8 on the PC connector 144A is connected to the CPU 140 and is arranged so that when the connect cable is plugged into the PC connector, the signal on pin 8 will be pulled low, signalling to the CPU 140 that a PC has been plugged in.

The selector circuit is arranged to select between PC input and RF receiver input under control of the CPU 140. When a PC is plugged into the system and the correct codes have been received from the PC, the system will accept parametric data for programming into the non-volatile memory area of the CPU 140. Thereafter, the system defaults to monitoring an infrared receiver unit 146 illustrated in Figure 4C. Communication with a GPS receiver is effected via an asynchronous serial link at pin 12 of the UART 144 and control/setup data is transmitted to the GPS from pin 10 of the UART 144. Communication with the RF receiver is effected from pin 3 of the RF receiver connector 144B via the level translator 144C and selector 145 to the UART at pin 20 on the CPU 140. In the event of a beacon

transmitter being implemented, communication with the RF transmitter is effected via an asynchronous serial link connected from pin 3 of the RF receiver connector 144B via the level translator 144C and selector 145 from the UART at pin 21 on the CPU 140.

A high current interface circuit 152 is used to enable the control circuit to drive relays RL6, RL7, RL8 and RL9. Relays RL6 and RL7 form part of the secondary immobilisation circuits used to immobilize the fuel solenoid or pump and the ignition circuit. The relay RL8 is used to power the vehicle horn or alarm, and the relay RL9 is activated once the vehicle is enabled, and is used to optionally cause the central locking system of the vehicle to be operated. The high current interface circuit 152 also connects the fibre optic cable 34 to a third immobilization circuit via a fibre optic link, which includes an HFBR 1521 transmitter 153, the fibre optic cable and an HFBR 2521 receiver.

The power supply circuitry of Figure 4B includes a first voltage regulator 158 which is used to convert the 13.8 volts DC from the vehicle power supply to 5 volts DC required by the CPU and the peripheral circuitry. A second voltage regulator 159 regulates the 5 volts down to 3.1 volts. This regulator has two sources of supply, namely the first regulator 158 and an external battery. The battery is a 4.2 volt battery, and is regulated down to 3.1 volts when power from the vehicle supply is removed. This allows for storage of information such as ignition status, door status and code status should the vehicle power supply be interrupted.

An under-voltage detection circuit is incorporated into the first voltage regulator 158. Pin 5 of the voltage regulator 158 causes the CPU 140 to be

re-set if the output voltage of the first voltage regulator 158 falls below 4.75 volts. The CPU 140 communicates with the infrared receiver unit 146 via RS485 interface IC's 164A and 164B, which link the CPU 140 to a micro-controller 165 at the heart of the receiver unit 146.

A polling opto-coupler 166A is similarly linked to the main CPU 140, and is used by the main CPU to initiate a polling signal informing the receiver unit that data is to be requested. A door switch opto-coupler 166B interfaces signals between the door switch and the micro-controller 165, and an ignition opto-coupler 166C interfaces signals between the ignition switch and the micro-controller 165. An optional brakepad opto-coupler 166D senses when the brake pad of the vehicle is activated. As was described previously in the specification, power is cut to the ignition on receipt of a signal from the transmitter only in the event of the brakepad having been activated.

A rolling code decoder 167, which incorporates an on-board memory within which coded parameters are stored, decodes data sent from a remote push button unit 168 of Figure 4D. A high current driver 170 is used to interface signals from the micro-controller to three LEDs, LD1, LD2 and LD3. LD1 is an infrared LED used to communicate data to the infrared remote push button 168, and LD2 and LD3 are indicator LEDs. An infrared receiver/amplifier 171 is used to receive data from the remote push button unit, and to convert it to an electrical signal via inverter 172 for decoding at the rolling code decoder 167. A regulator 173 is used to convert the 13.8 volts from the vehicle power supply to the 5 volts required by the circuitry. An undervoltage detector 174 also forms part of the power supply circuitry, and is used to provide a clean reset to the circuitry when power is supplied.

When a door of the vehicle is opened, the micro-controller 165 sends an activation signal to the remote push button unit 168 via infrared LED LD1. Digital divider circuits 175A and 175B, in conjunction with gate 175C, form a divider chain to generate a 38 kHz squarewave carrier signal which is modulated by the micro-controller 165 so as to form an infrared signal which is transmitted to the infrared remote push button 168. The remote push button responds by transmitting a rolling code to the infrared receiver/amplifier 171. The micro-controller retransmits this rolling code to the remote push button unit 168 and waits for the same code to be returned. When this occurs, the micro-controller checks to see if the driver-activated alarm is present. If so, a flag is set up in the software, together with a valid code flag. The micro-controller 165 accordingly checks to see if the ignition is switched on or off, as a result of which a flag is respectively set or cleared. The bitstream for the main control unit 140 is set up according to the flags, and the micro-controller unit 165 waits to be polled by the main control unit. The data is transmitted to the main control unit, which then uses this data to perform its functions according to the flowchart of Figure 5.

The push button unit 168 illustrated in more detail in Figure 4D includes a micro-controller 180 which is coupled to a rolling code generator 182 which generates an apparently random code each time it is activated. A 3.6 volt battery supplies power to the circuitry. An infrared receiver/amplifier module 186 receives data from the infrared receiver unit illustrated in Figure 4C. A resistor/capacitor circuit 187 is connected to pin 1 of the micro-controller 180, and provides a clean re-set when the battery is first connected. An infrared LED L1 is used to communicate data to the infrared receiver unit. A switch S1 is used to initiate the driver activated alarm

condition described earlier on in the specification.

Digital divider circuits 185A and 185B, together with gate 185C, forms a divided chain to generate a 38 kHz squarewave carrier signal which is modulated by the rolling code decoder 182 to form the infrared signal which is transmitted to the infrared receiver of Figure 4C. The signal is gated and buffered by gate 185D.

When the receiver 186 receives an activation signal from the infrared receiver unit, the micro-controller 180 sets up a code on output pins PC1 and PC0. This in turn activates the rolling code generator 182, which transmits an apparently random code to the infrared receiver. An inter-frame delay follows during which time the infrared receiver retransmits this code, which is received by the receiver 186. The micro-controller 180 checks that the data is the same as that which was transmitted, and if the codes match, the micro-controller keeps the rolling code generator 182 activated for one more frame. This confirms to the infrared receiver that the transaction was completed.

If the switch S1 is pressed, a different code is set up on the output pins PC0 and PC1 of the micro-controller. The general sequence is substantially identical to that described above, and the infrared receiver decodes a different data code, after which the driver-activated alarm mode is entered.

At the end of the transaction, the micro-controller unit 165 signals the main CPU 140 via the synchronous serial link. The main CPU, which serves as a control unit then disables the immobiliser circuitry, allowing the vehicle to be started. As was described previously, there are two separate sub-codes

in the data sent from the infrared push button. The first code signals normal operation, and a second code signals a driver-activated alarm mode. In both cases, the vehicle may be started and driven. On receipt of the second code, the control unit activates the beacon transmitter which enables the vehicle to be tracked.

Once the vehicle has been started, and if the driver's door is subsequently opened, the infrared receiver signals the control unit 140 which then activates the RF receiver 60. This step is defined as arming the immobiliser. Should the vehicle then drive past a roadside transmitter, the RF receiver receives coded data from the transmitter and relays it to the control unit which then enables the immobilisation circuitry, causing the vehicle to stop. This procedure will not occur if the driver-activated alarm mode is active.

It is possible to specifically disable the vehicle from the driver-activated alarm mode by sending the specific identity code for that particular vehicle via an RF transmitter. This procedure would be initiated by authorised security personnel once the driver of the vehicle was no longer in danger.

The basic operation of the main system is illustrated in the flowchart of Figure 5, the contents of which are self-explanatory. When the system is first powered up, a system start sequence is performed, which initialises all the processor registers and memory locations. The system peripherals are also initialised, including the infrared receiver unit, (also referred to as the DASHBOARD unit), the DUART and the RF receiver and transmitter (if installed). The system powers up in the immobilised mode.

The Dashboard unit is polled and it sends back a bit stream that carries data

relating to the status of the door, ignition and remote push-button. The system first checks if the door is open. If so, the immobiliser is armed. This is unconditional, and any time the door is opened the immobiliser progresses to the armed mode.

If the door is not open the system checks if a valid code has been received from the remote push-button. If so, the immobiliser is disarmed. All alarms, immobilisation and arming are cancelled. At this point the system checks to see if a driver-initiated alarm is present, and if so, the beacon transmitter is activated. The vehicle may still be driven, but the beacon transmitter will enable the vehicle to be tracked. If the door is opened while this mode is active, the immobiliser becomes armed, but the beacon transmitter is not disabled until a valid code is received from the remote push-button.

If no valid code has been received from the remote push-button the system checks to see whether the ignition is on. If so, the immobiliser is armed. The system then checks to see if a valid code has been received by the RF receiver unit. If so, the vehicle is immobilised. If the ignition is not on the vehicle is simply immobilised from the beginning - this is the anti-theft aspect of the design. This program sequence loops continuously.

Referring now to Figure 6A, a fourth embodiment of a vehicle security system 190 includes a control unit in the form of a micro-controller 192 which is arranged to receive information from three sources, namely a first opto-coupler IC 194 for interfacing to the ignition switch, a second opto-coupler IC 196 for interfacing to the door switch, and a rolling code decoder 198 which interfaces to an infrared receiver IC 200 via an inverter 202. The

micro-controller 192 processes the information from these three sources and generates outputs to an indicator circuit 204 and to a fibre optic transmitter IC 206 via a high current interface driver 208. The micro-controller 192 is provided with a crystal oscillator 210, and is powered via a voltage regulator 212.

Figure 6B illustrates a remote push-button key which serves to disarm the security system. The push-button key 214 is provided with a rolling code generator 216, which drives an infrared transmitting LED 218 via a square-wave oscillator 220 and an inverter 222. When either of switches 224 and 226 are operated, the rolling code generator 216, which is powered by means of a 3.6 volt lithium cell battery 228, is activated. Once activated, the rolling code generator 216 generates a coded pulse train on its output pin 1. This pulse train is fed to the gating input of the squarewave oscillator 220. When this input is high, the oscillator is enabled and a squarewave is generated at its output. This frequency of the signal is dependent on the time constant determined by capacitor 228 and resistor 230, and is nominally 38kHz. This signal is inverted and is fed to the inverting buffer formed by inverter 222. The LED 218 transmits an infrared optical signal which is received at the infrared receiver 206 illustrated in Figure 6A.

The operation of the vehicle security system of Figure 6A and 6B will now be described with reference to the flowchart illustrated in Figure 7. On being powered up, the micro-controller 192 checks the inputs from the ignition switch 194, the door switch 196 and the rolling code decoder 198. At turn on, the micro-controller causes the immobilising circuit to default into the immobilised state, which is indicated when the red LED 204A is illuminated. When the driver pushes the remote push button transmitter 214,

a coded infrared signal is received by the infrared receiver 206. The output from the receiver is inverted at the inverter IC 202, from where it is conveyed to the rolling code decoder 198. If the signal is valid, the output of the rolling code decoder goes low and these low signals are in turn conveyed to input pins 9 and 10 of the micro-controller 192. The micro-controller processes these inputs, together with the inputs from the ignition and door switches 194 and 196. If the door is closed, the ignition switch is off and the received code is valid, the micro-controller will transmit the coded data to the fibre optic transmitter 206 via the high current interface driver 208. The micro-controller will also turn off the red LED 204A and will activate the green LED 204B. The fibre optic transmitter is in turn linked to an infrared receiver unit which is essentially identical to that illustrated at 146 in the previous embodiment.

If the driver does not turn on the ignition switch within 30 seconds of opening the vehicle door, the micro-controller will cause the vehicle to be immobilised, thereby preventing the vehicle from remaining in the disarmed state for too long. When the ignition is turned off, the micro-controller waits until the door is opened. As soon as this happens, the micro-controller stops sending coded data to the fibre optic transmitter 206, which causes the vehicle to be immobilised. If the door is not opened within 30 seconds of the ignition being switched off, the micro-controller will immobilise the vehicle in any event for the same reason as above.

An advantage of using a fibre optic cable is that it is almost impossible to splice the optical cable once it has been cut. Further, the optical cable cannot be bypassed, as both the transmitter and receiver units are encapsulated, and the receiver unit can only be activated by means of a

characteristic optical signal having the exact predetermined code and carrier frequency. If the optical cable is rejoined to another light source, the source will have to be at exactly the right modulating frequency in order to enable the fuel solenoid. This is made even more difficult in the case of a coded modulating signal. Further, the rejoining procedure will have to be "seamless", in that any discontinuity in the transmission of the coded optical signal will activate the immobiliser.

CLAIMS

1. A vehicle security system comprising a control circuit, a first enabling/disabling circuit remote from the control circuit and being arranged to immobilise the vehicle, a first optical link extending between the control circuit and the first enabling/disabling circuit, and enabling means for enabling the enabling/disabling circuit via the first optical link, the enabling means including enabling signal generating means for generating a first characteristic enabling signal for continuous transmission via the first optical link, whereby the enabling/disabling circuit is arranged to immobilise the vehicle on non-receipt of the first characteristic enabling signal.

2. A vehicle security system according to claim 1 in which the enabling means includes coded entry means for generating a second coded enabling signal, the enabling signal generating means being responsive to the second coded enabling signal.

3. A vehicle security system according to claim 2 comprising first sensing means for sensing an act of entry into or exit from the vehicle, the control circuit including first arming means responsive to the first sensing means for preventing the first enabling signal generating means from responding to the second coded enabling signal.

4. A vehicle security system according to either one of claims 1 or 2 comprising first sensing means for sensing an act of entry into exit

from the vehicle, the control circuit including first arming means responsive to the first sensing means for arming the enabling/disabling circuit via the control circuit such that the vehicle is in an armed mode in which it is able to respond to a remote disabling signal, but can still be driven.

5. A vehicle security system according to claim 3 or 4 which includes second sensing means for sensing the activating of the vehicle, the first arming means also being responsive to the second sensing means.

6. A vehicle security system according to any one of the preceding claims 3 to 5 in which the first sensing means is arranged to sense the opening of a door of the vehicle.

7. A vehicle security system according to either one of claims 4 or 5 in which the second sensing means is arranged to sense the turning on of the vehicle ignition switch.

8. A vehicle security system according to any one of the preceding claims in which the enabling signal generating means includes modulating circuitry for generating a characteristic modulated or coded optical signal as an enabling signal, and the first enabling/disabling circuit includes detection circuitry arranged to respond only to the characteristic modulated or coded signal.

9. A vehicle security system according to any one of the preceding claims which includes a second enabling/disabling circuit remote

from the control circuit and being arranged to immobilise the vehicle, and a second optical link extending between the control circuit and the second enabling/disabling circuit.

10. A vehicle security system according to claim 9 in which the first and second optical links include first and second fibre optic cables, first and second optical transmitters and first and second optical receivers.

11. A vehicle security system according to claim 5 in which the control circuit includes logic means for enabling the enabling signal generating means only in the event of the first arming means not having responded to both the first and second sensing means.

12. A vehicle security system according to claim 11 in which the logic means includes timing means for timing a delay between receipt of an arming signal from the first sensing means and the receipt of an arming signal from the second sensing means, the logic means being arranged to immobilise the vehicle in the event of the delay exceeding a predetermined time period.

13. A vehicle security system according to claim 12 in which the timing means is arranged to time a delay between non-receipt of an arming signal from the second sensing means and receipt of an arming signal from the first sensing means, the logic means being arranged to immobilise the vehicle in the event of the delay exceeding a predetermined time period.

14. A vehicle security system according to claim 4 which includes a

receiver for receiving the remote disabling signal from a remote transmitter unit, the first arming means including a primary immobilising circuit arranged to immobilise the vehicle on receipt of the disabling signal.

15. A vehicle security system according to claim 14 in which the primary immobilising circuit is responsive to the disabling signal to immobilise the vehicle only in the event of the primary immobilising circuit being armed via the first arming means.

16. A vehicle security system according to claim 15 which includes second sensing means for sensing the activating of the vehicle, the first arming means being responsive to the first and second sensing means, and the control means being arranged to arm the primary immobilising circuit for receipt of a remote disabling signal in the event of the first arming means having responded to the first and second sensing means.

17. A vehicle security system according to any one of claims 9 to 10 in which the first and second enabling/disabling circuits are arranged to selectively disable the vehicle by cutting off the fuel supply via a solenoid-operated fuel valve, to disable the vehicle ignition system, disable a starter motor, or disable an automatic transmission system.

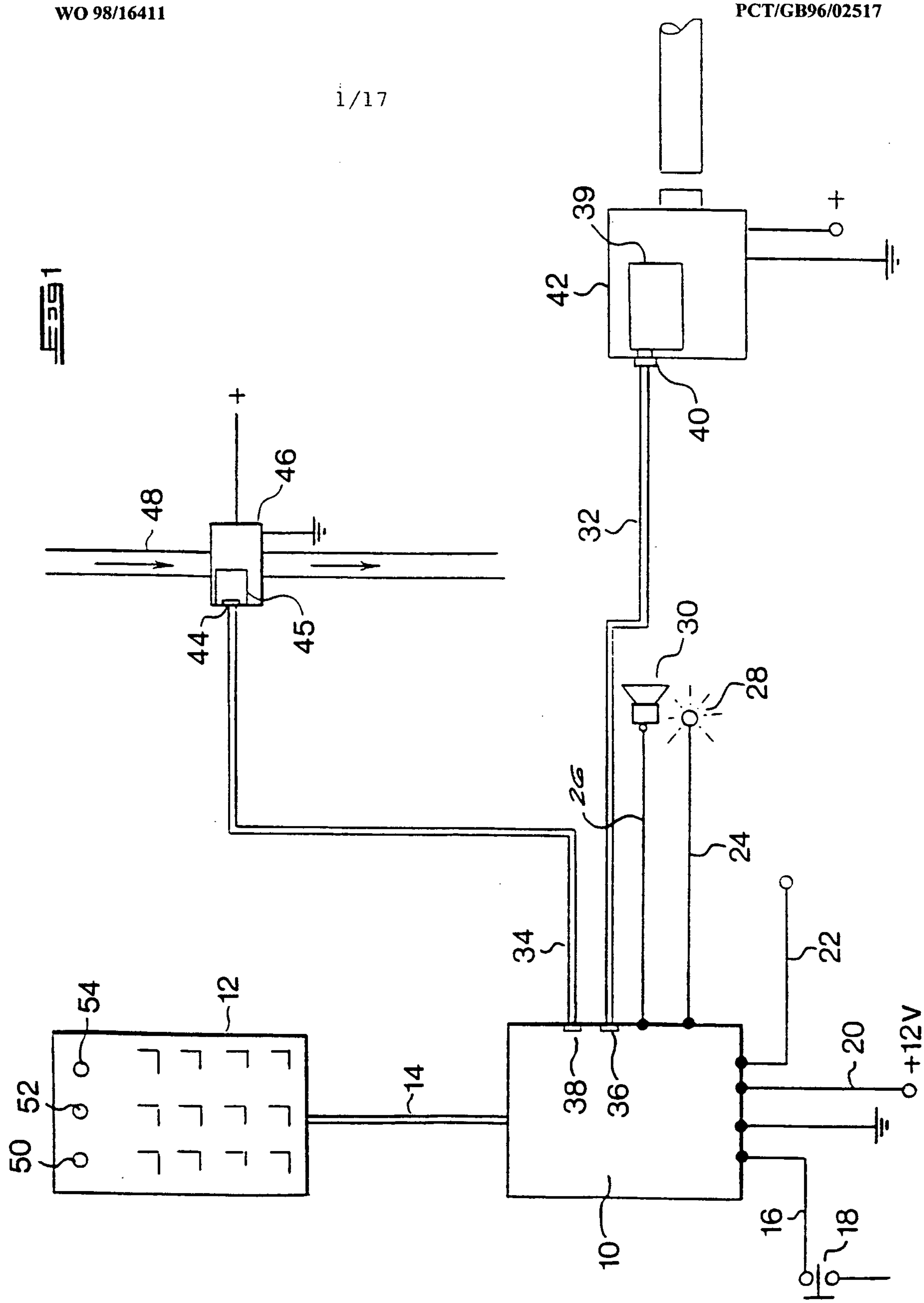


FIG 1
10
12
14
16
18
20
+12V
22
24
26
28
30
32
34
36
38
39
40
42
44
45
46
48
50
52
54

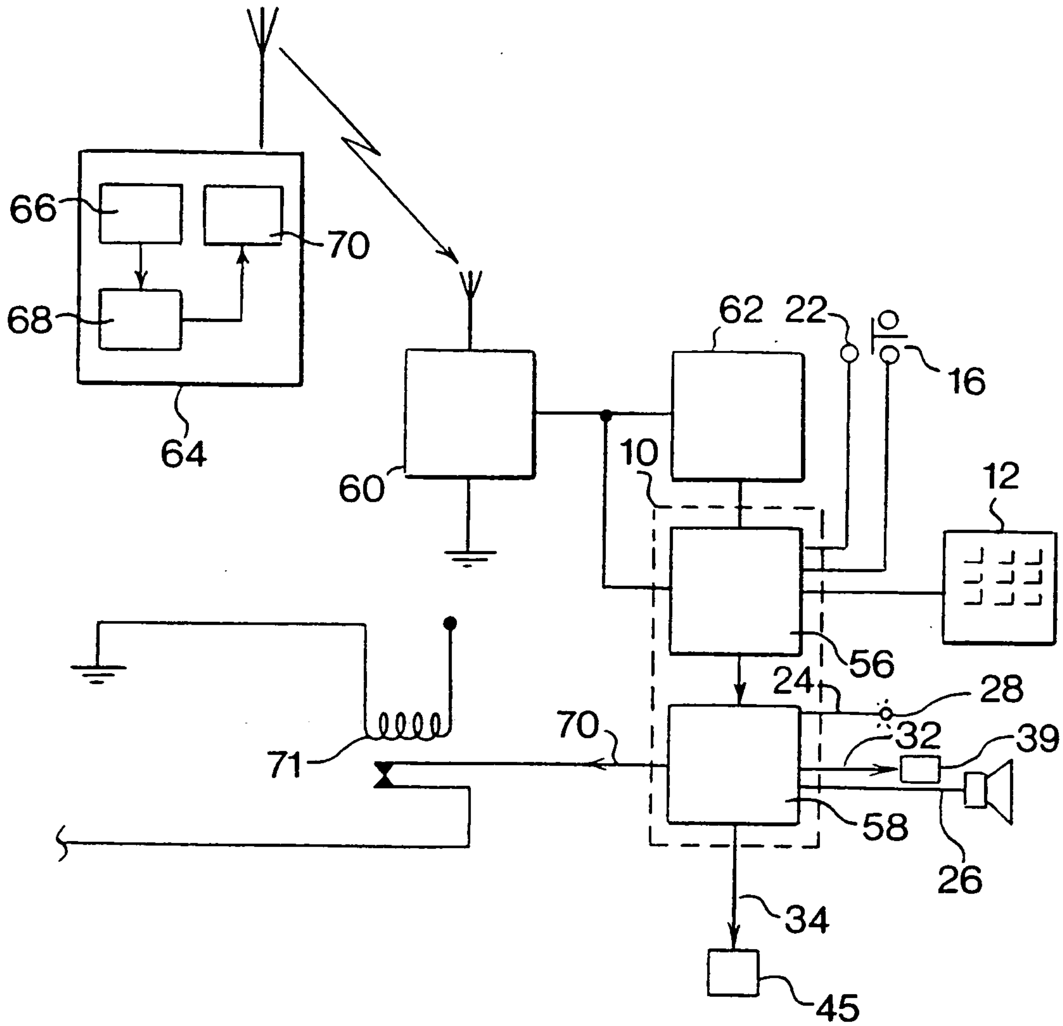
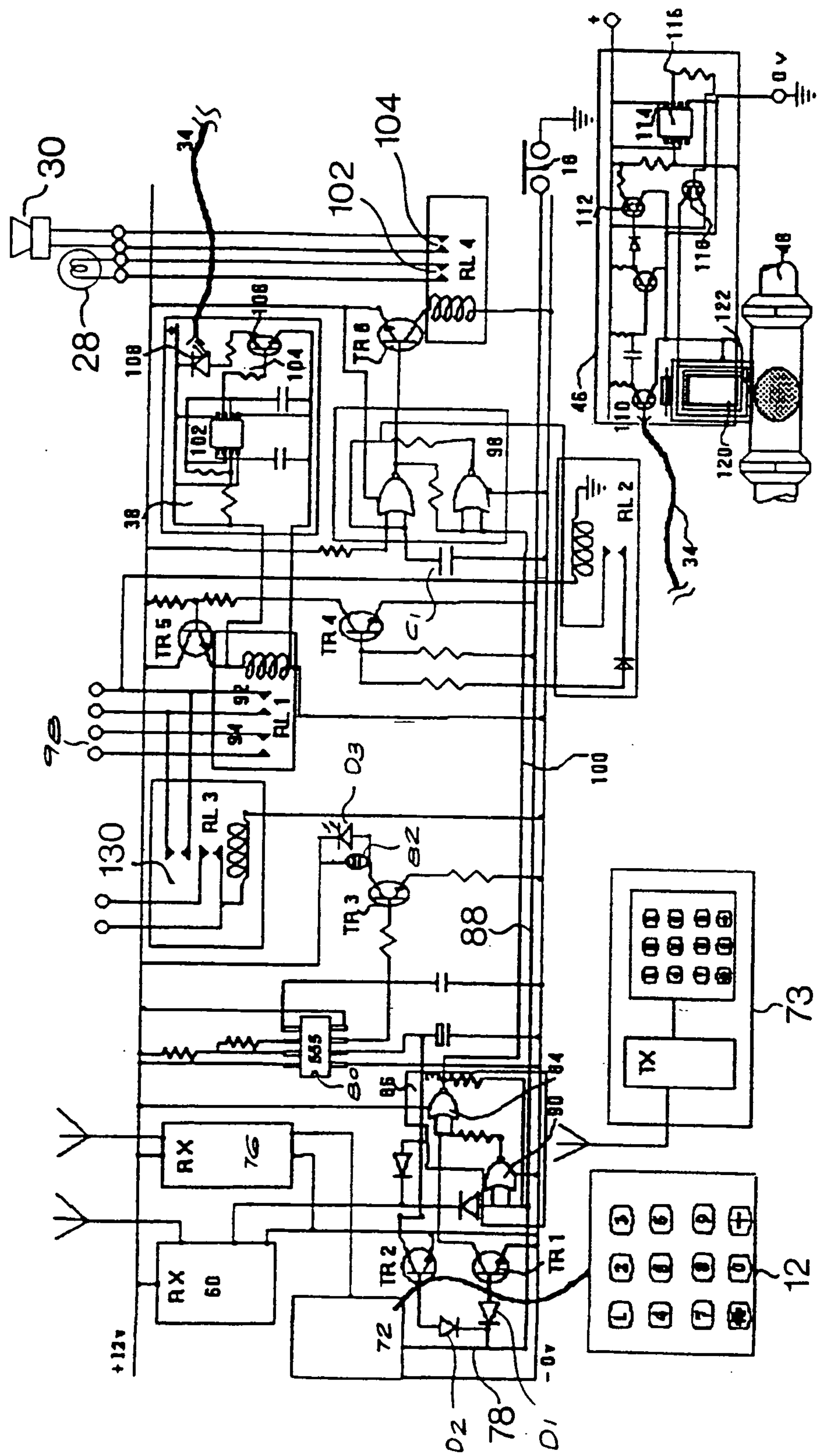


FIG 2


RX
60
RX
76
TX
73
12
555
80
TR 1
TR 2
TR 3
TR 4
TR 5
TR 6
RL 1
RL 2
RL 3
RL 4
+12v
-0v
0v
28
30
34
38
46
48
72
78
84
86
88
90
92
94
96
98
100
102
104
106
108
110
112
114
116
118
120
122
130
D1
D2
D3
C1

3

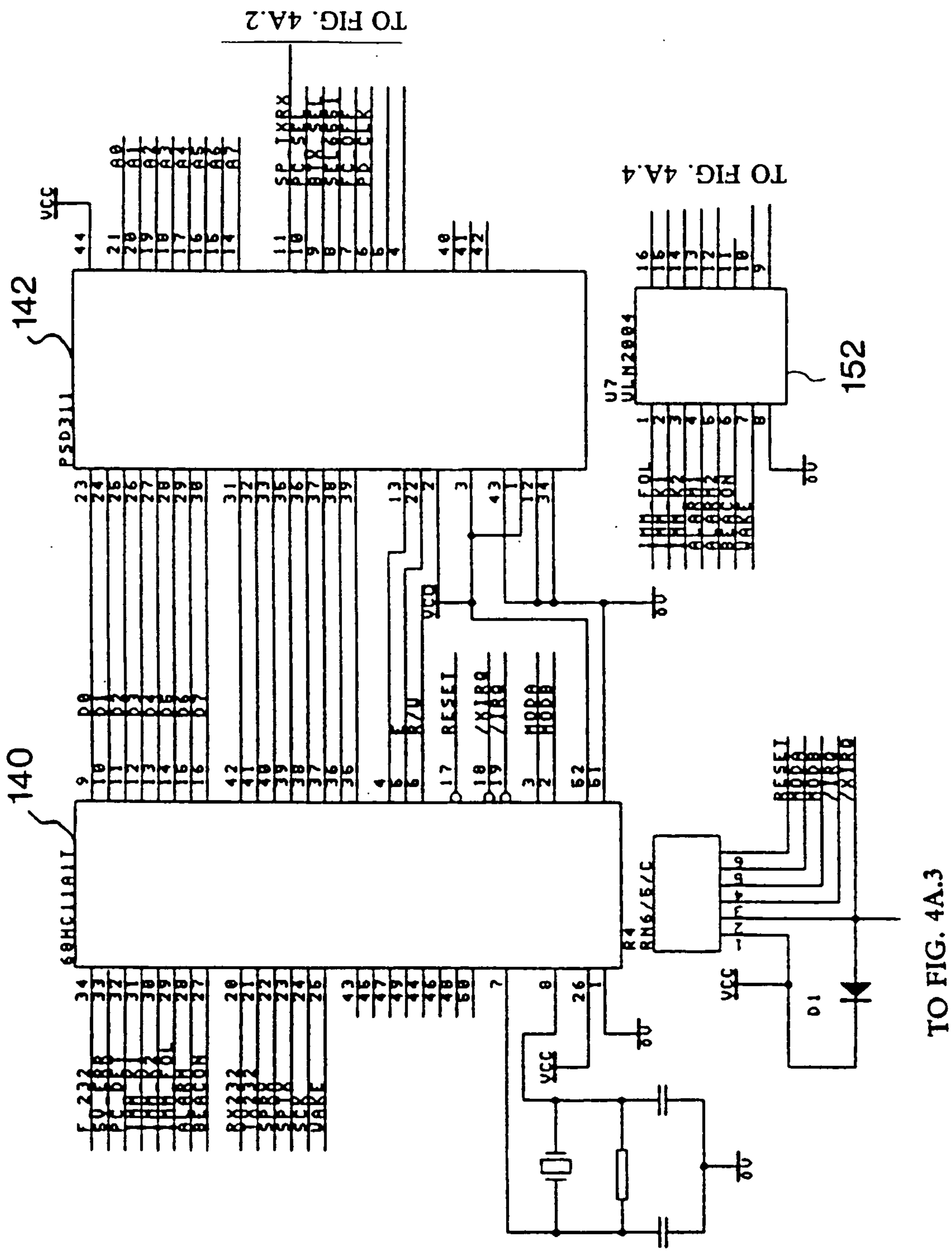

TO FIG. 4A.2
TO FIG. 4A.4
TO FIG. 4A.3
142
140
152
PSD311
68HC11A1T
U7
ULN2004
R4
RN6/5/C
D1
VCC
RESET
MODA
MODB
/IRQ
/XIRQ
R/W

FIG. 4A-1

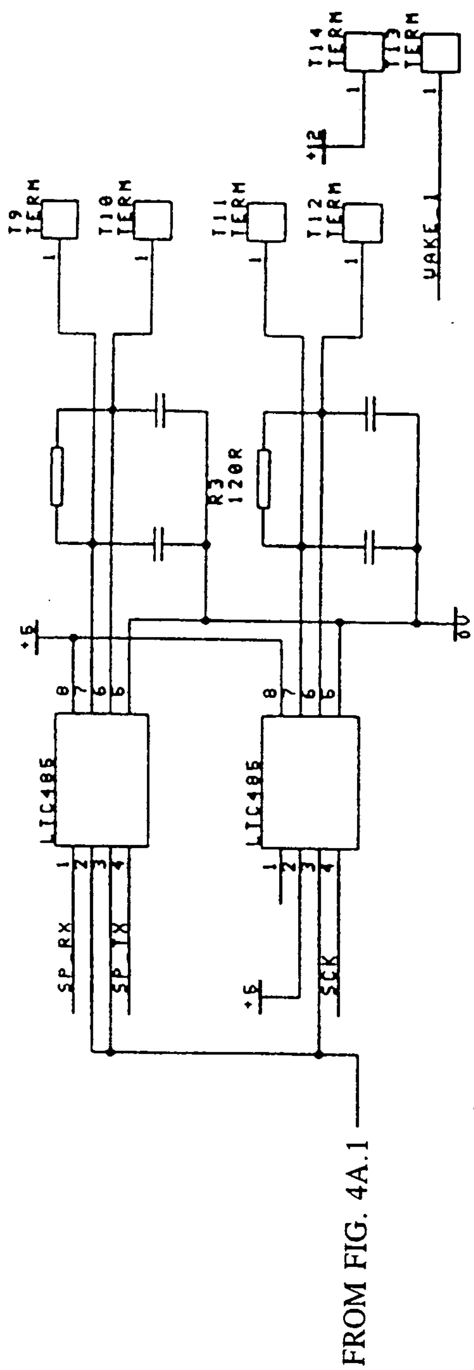

T9 TERM
T10 TERM
T11 TERM
T12 TERM
T13 TERM
T14 TERM
+12
WAKE 1
R3 120R
+5
0V
LTC485
LTC485
SP RX
SP TX
+5
SCK
FROM FIG. 4A.1

FIG. 4A·2

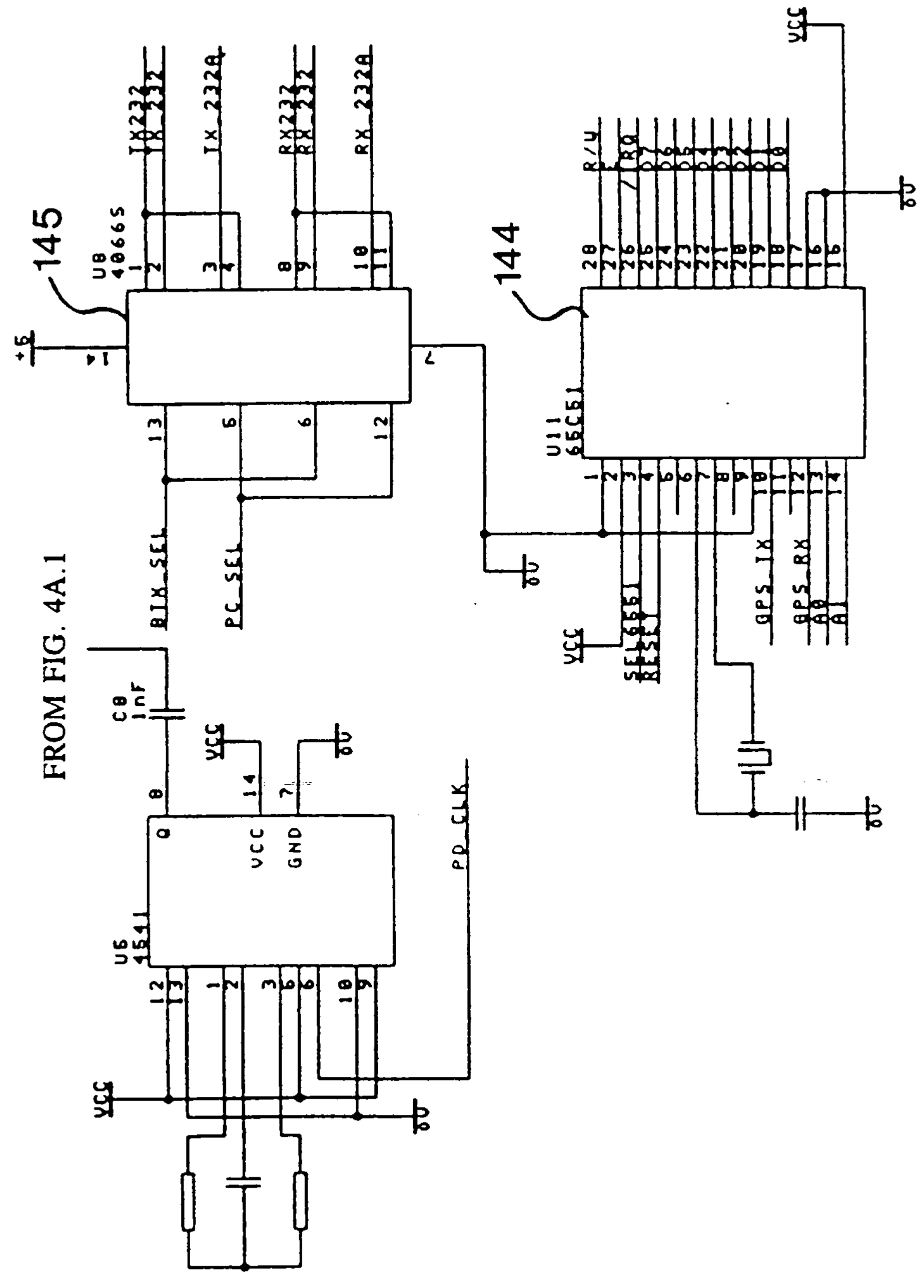

FROM FIG. 4A.1
145
144
U8
4066S
U11
65C51
U6
4541
C8
1nF
VCC
0V
+5
TX232
TX_232A
RX232
RX_232A
BIX_SEL
PC_SEL
PD_CLK
GPS_TX
GPS_RX
R/W
IRQ
RESET
Q
GND

FIG 4A·3

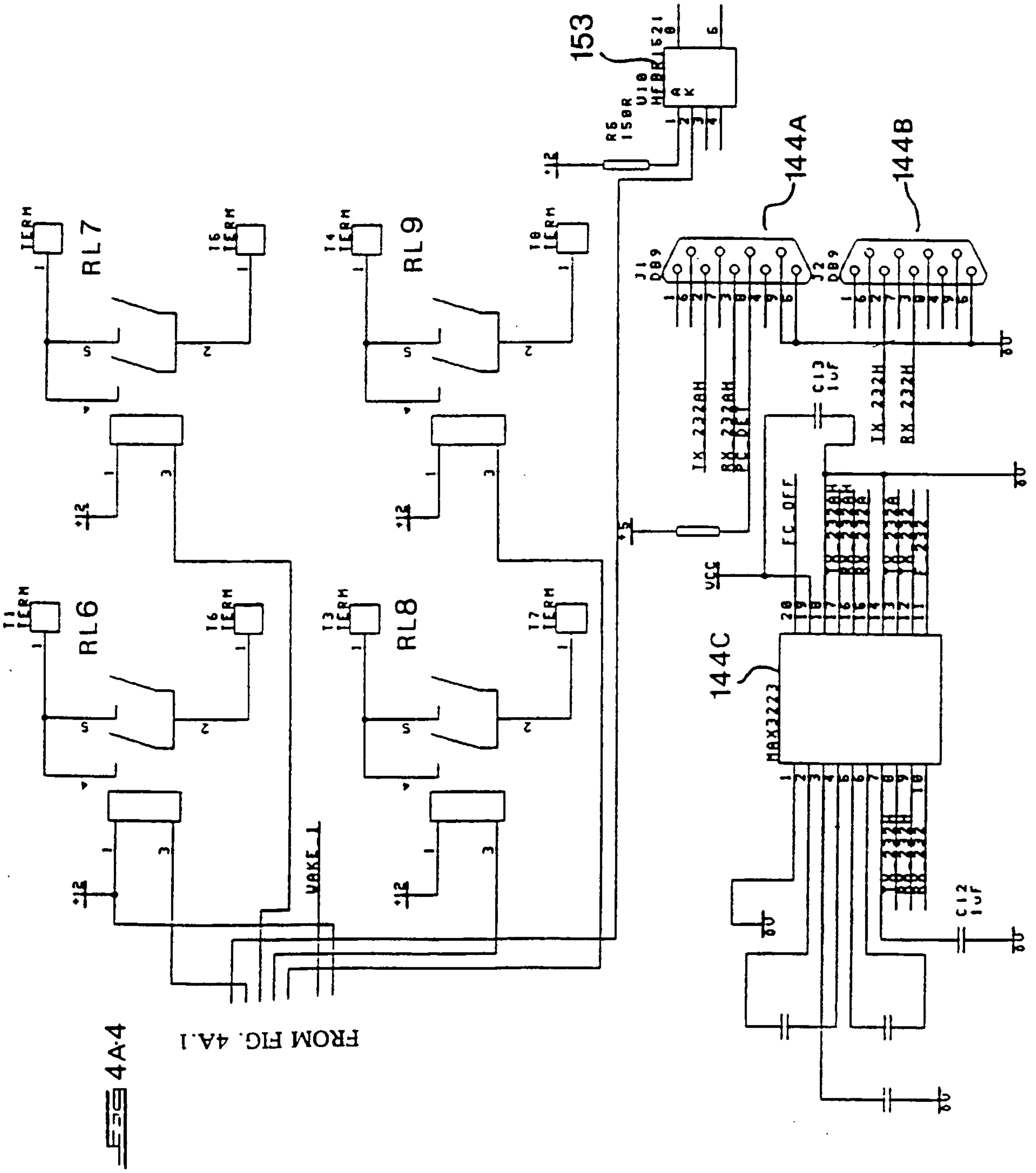


FIG. 4A·4

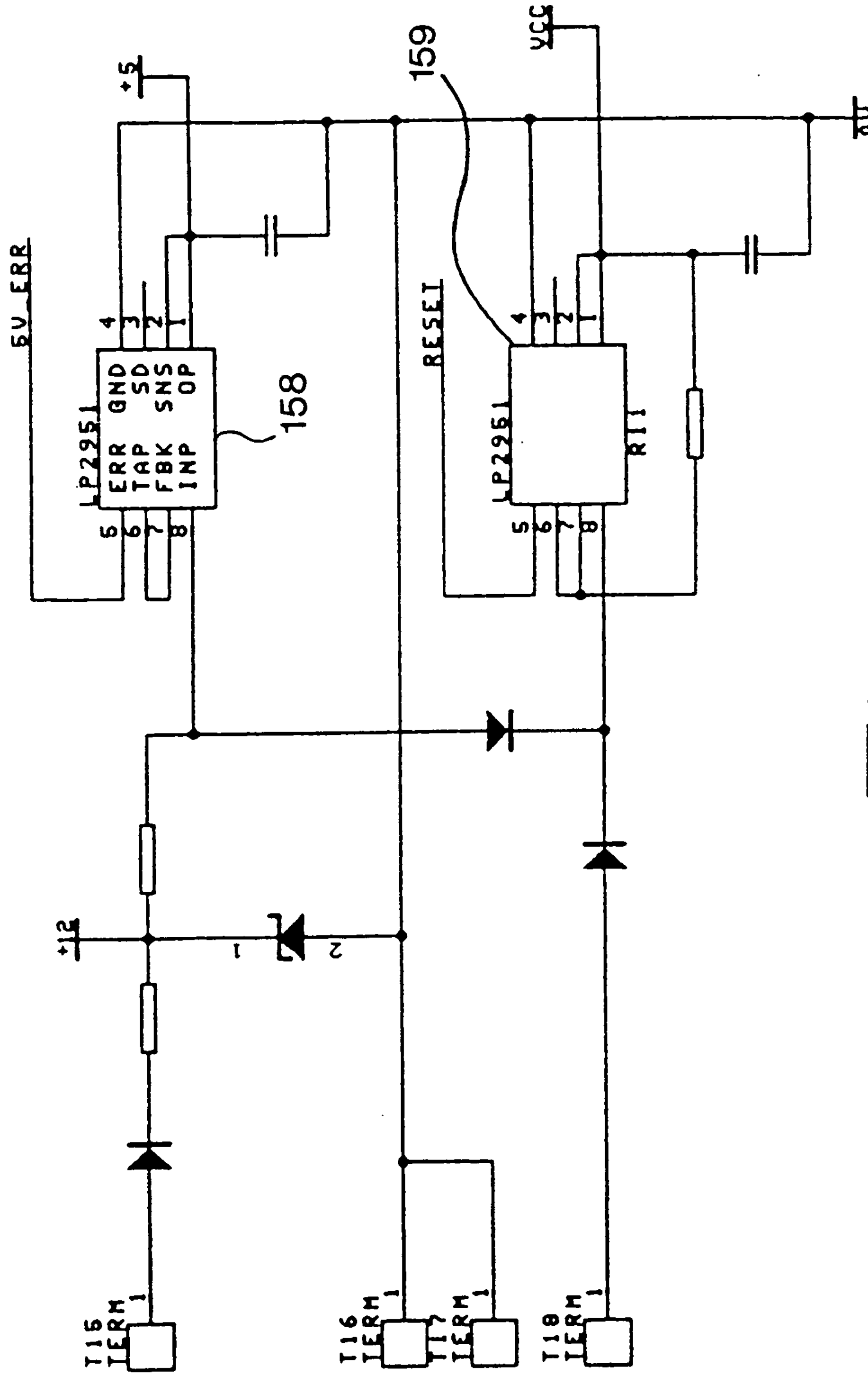

+5
VCC
0V
159
158
5V_ERR
RESET
LP2951
ERR TAP FBK INP
GND SD SNS OP
R11
+12
T16 TERM
T17 TERM
T18 TERM

FIG 4B

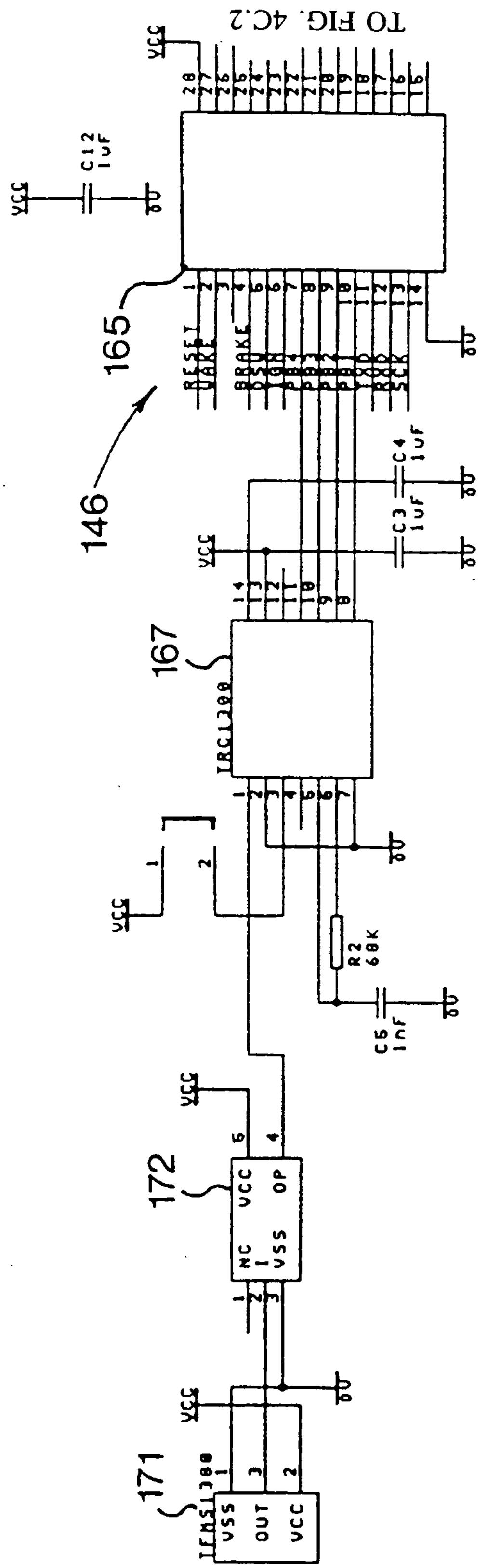

TO FIG. 4C.2
VCC
C12 1uF
165
146
RESET
BRAKE
C4 1uF
C3 1uF
167
R2 68K
C6 1nF
172
VCC
OP
NC
VSS
171
VSS
OUT
VCC

FIG. 4C-1

FIG 4C·2

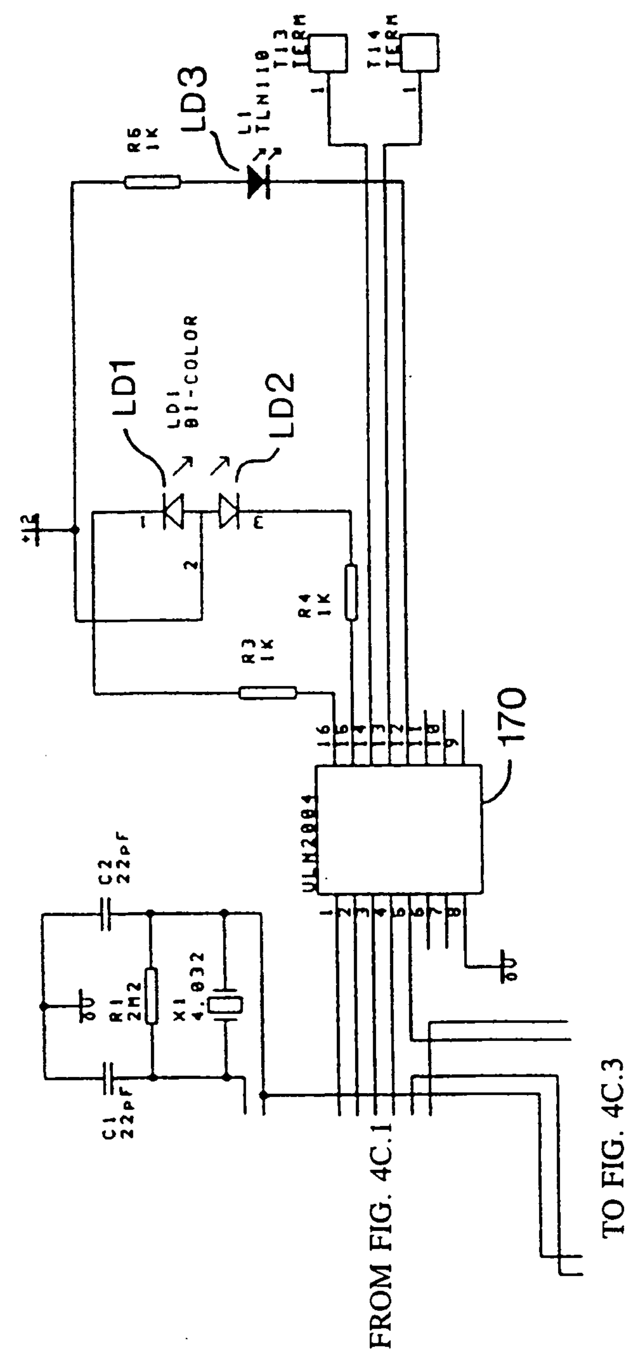
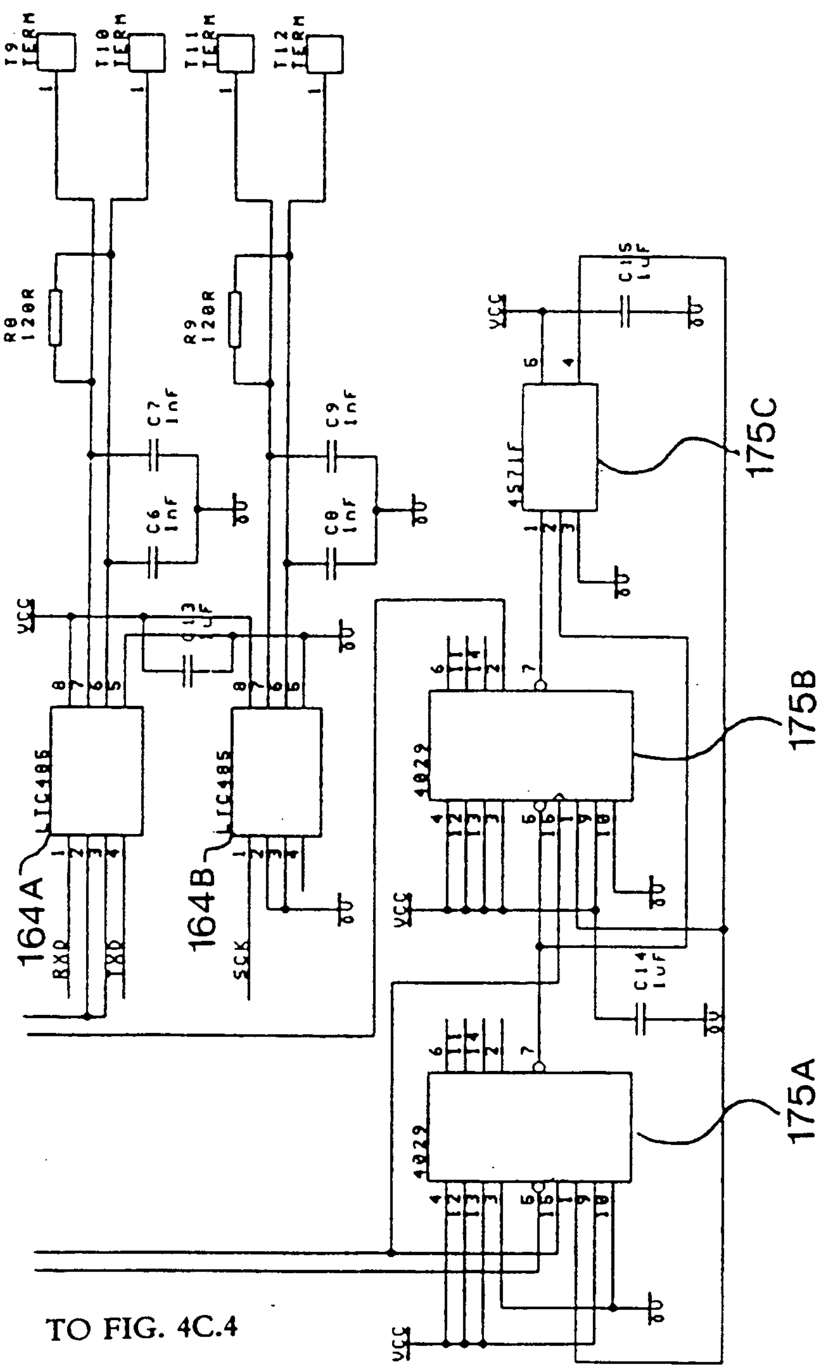

LD1
LD1 BI-COLOR
LD2
LD3
L1 TLN110
R6 1K
R4 1K
R3 1K
T13 TERM
T14 TERM
ULN2004
170
C1 22pF
C2 22pF
R1 2M2
X1 4.032
FROM FIG. 4C.1
TO FIG. 4C.3

FIG 4C·3


FROM FIG. 4C.2
TO FIG. 4C.4
164A
164B
175A
175B
175C
LTC485
4029
4571F
R8 120R
R9 120R
C6 1nF
C7 1nF
C8 1nF
C9 1nF
C13 1uF
C14 1uF
C15 1uF
T9 TERM
T10 TERM
T11 TERM
T12 TERM
RXD
TXD
SCK
VCC
0V

FROM FIG 4C.3

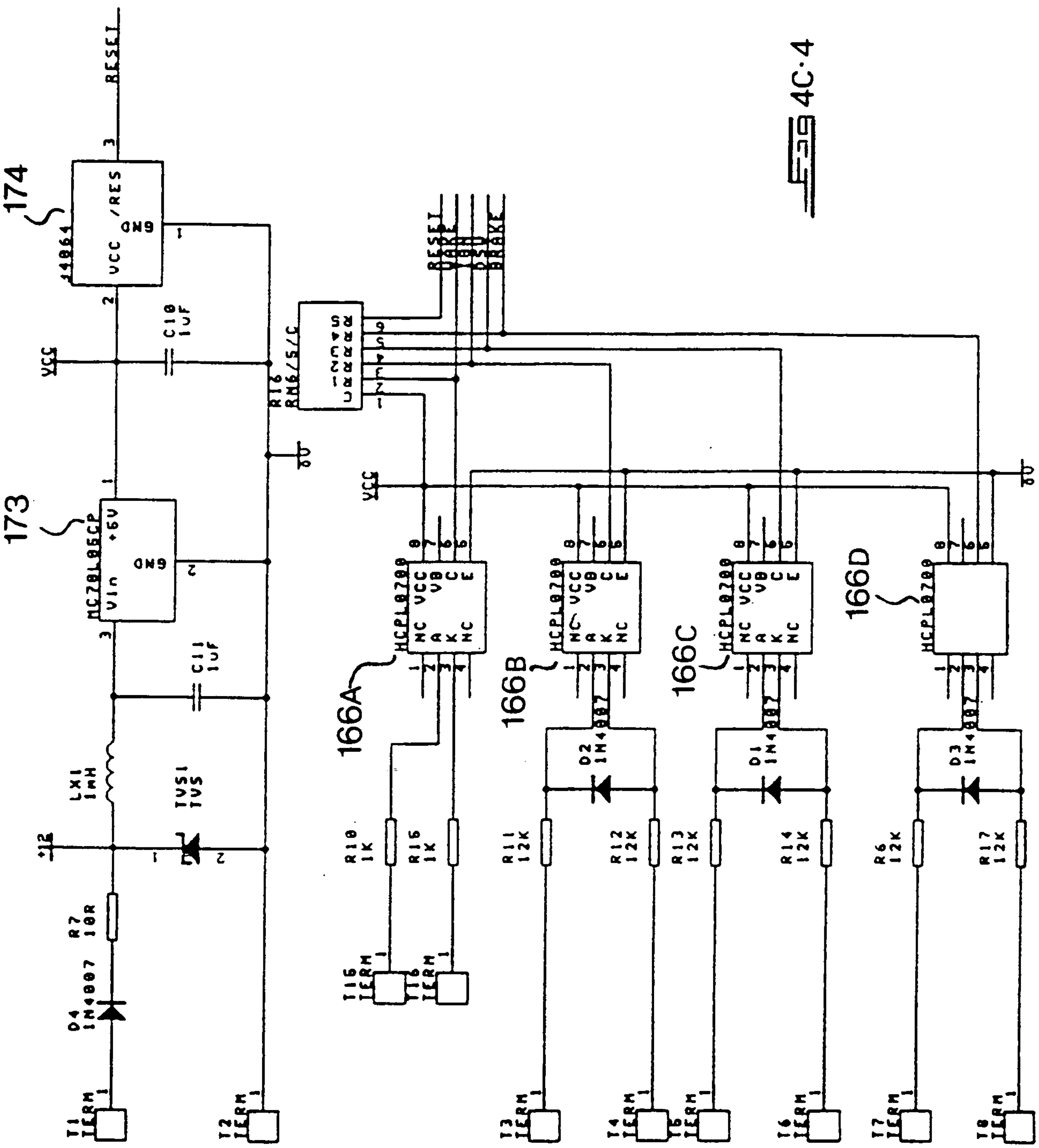


FIG 4C·4

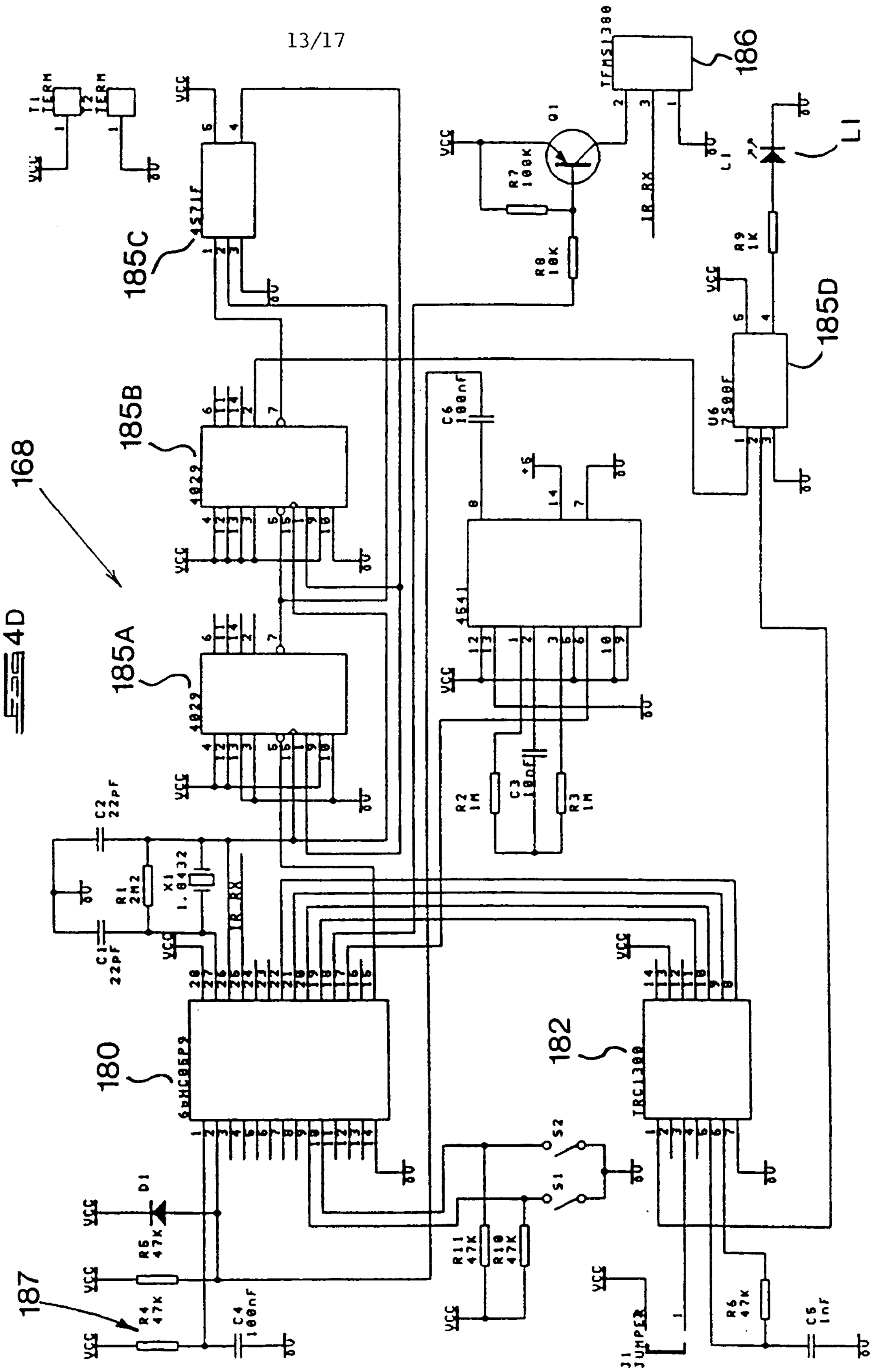


FIG 4D
168
180
182
185A
185B
185C
185D
186
187
L1
4029
4541
TRC1380
TFMS1380
VCC
0V

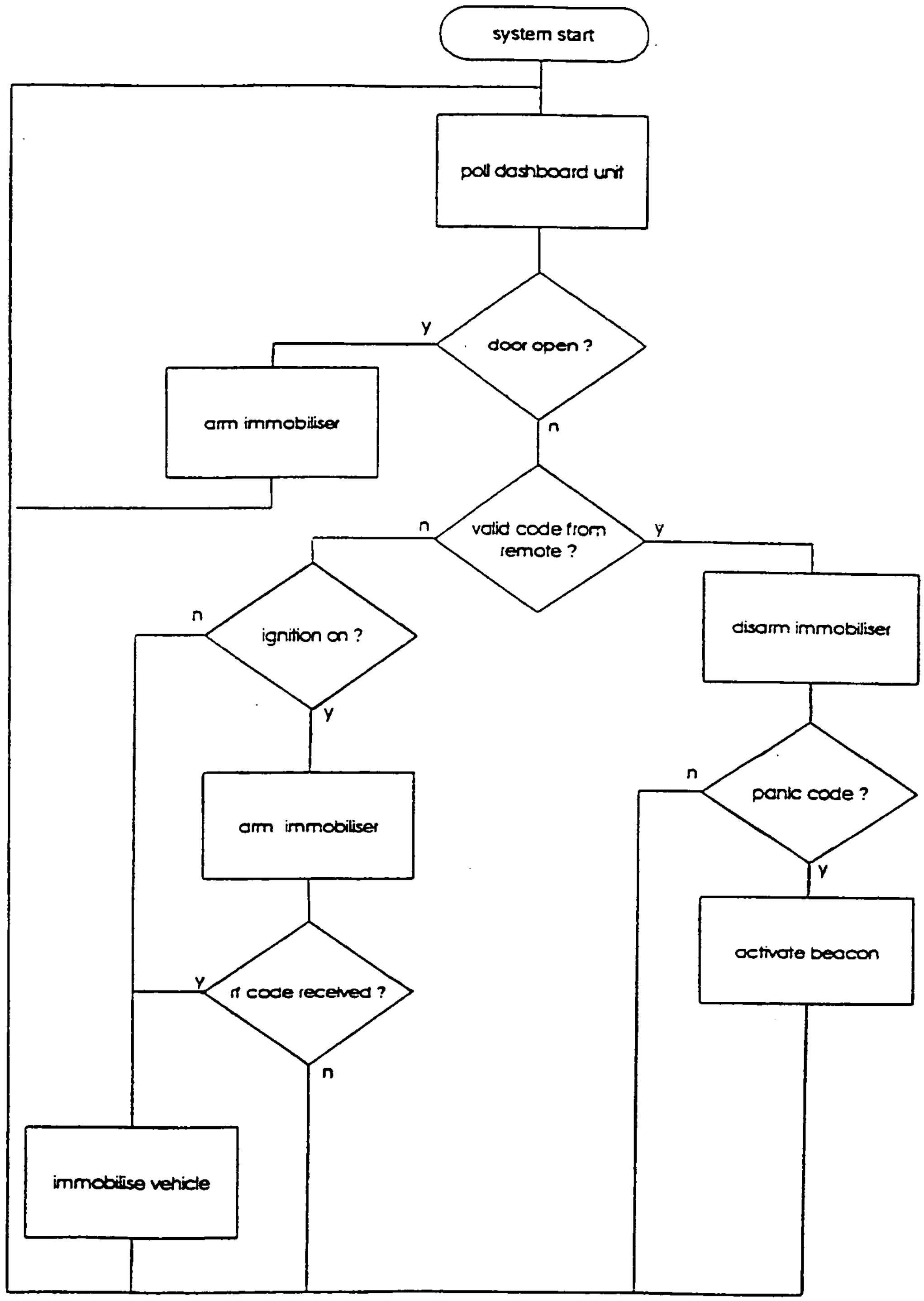
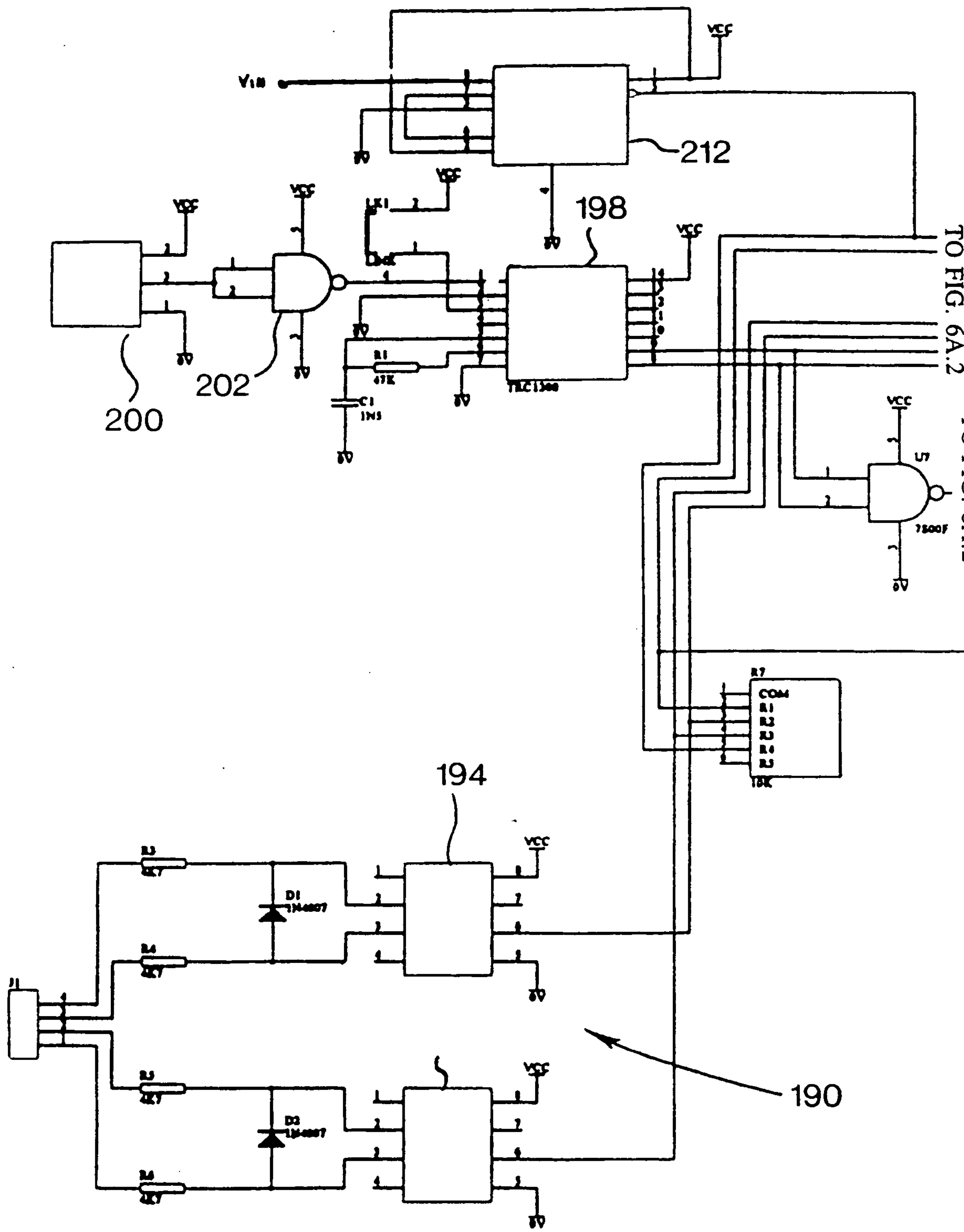

system start
poll dashboard unit
door open ?
y
arm immobiliser
n
valid code from remote ?
n
y
ignition on ?
n
y
disarm immobiliser
arm immobiliser
panic code ?
n
y
rf code received ?
y
n
activate beacon
immobilise vehicle

FIG 5



VCC
VIN
212
198
200
202
LK1
R1
47K
C1
1N5
0V
TLC1300
TO FIG. 6A.2
TO FIG. 6A.2
U7
7800F
R7
COM
R1
R2
R3
R4
R5
10K
194
R3
4K7
R4
4K7
R5
4K7
R6
4K7
D1
1N4007
D2
1N4007
J1
190

FIG 6A-1

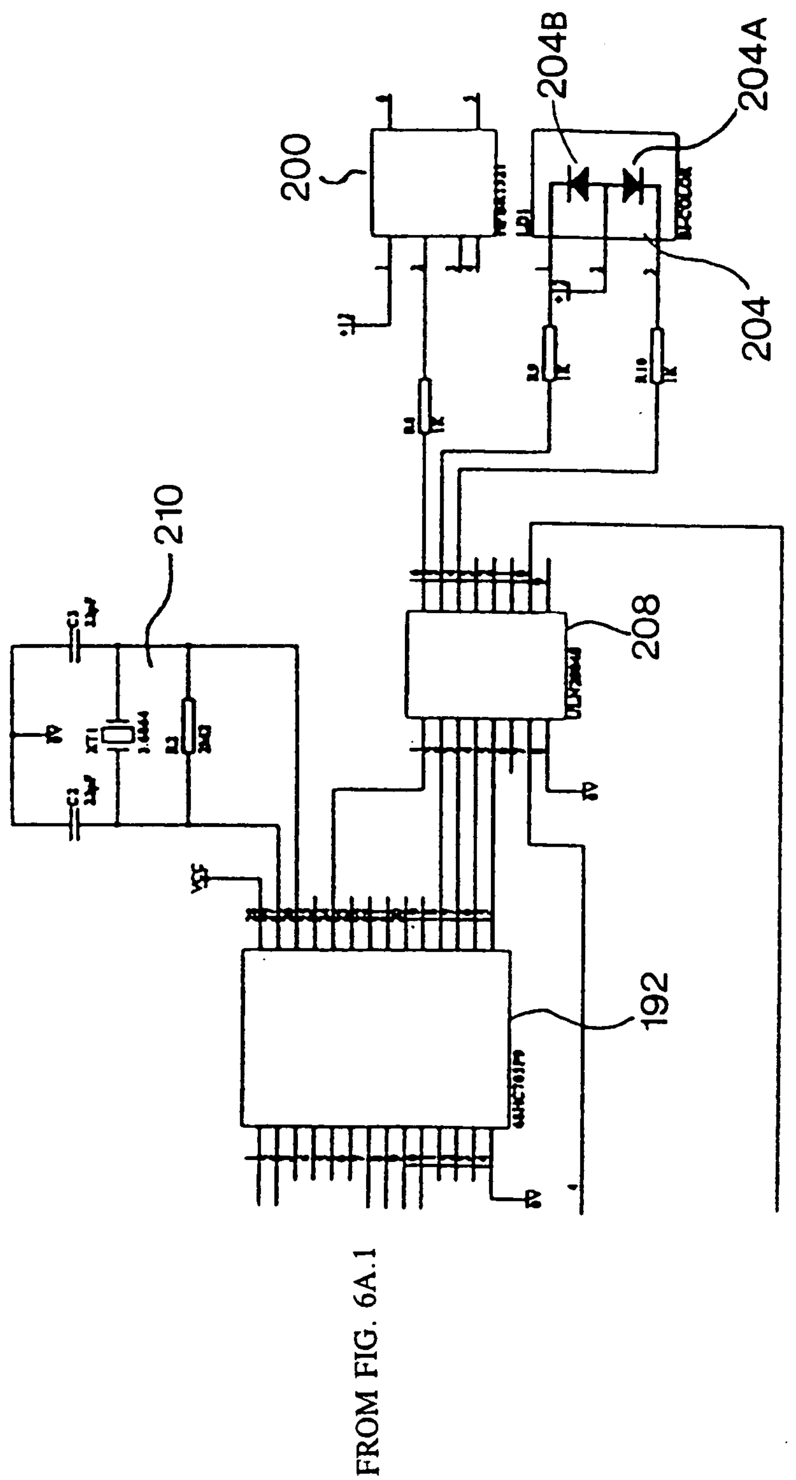


FIG. 6A:2

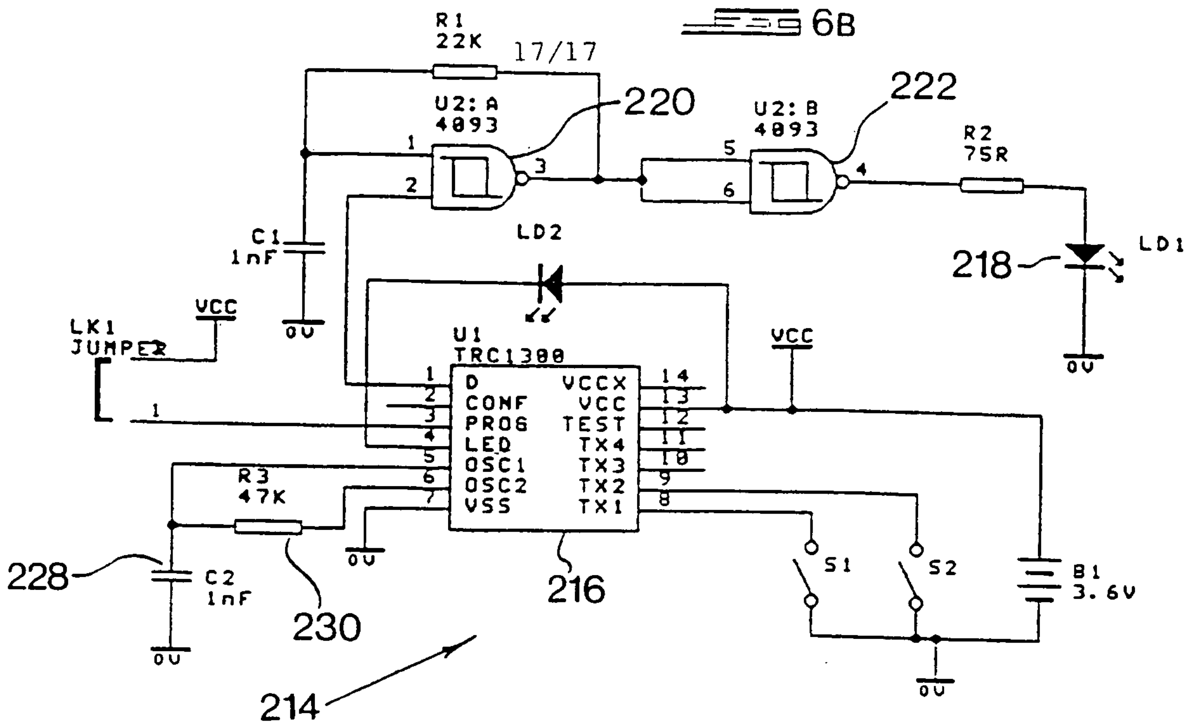

R1
22K
U2:A
4093
220
U2:B
4093
222
R2
75R
LD2
LD1
218
C1
1nF
VCC
LK1
JUMPER
0V
U1
TRC1300
D
CONF
PROG
LED
OSC1
OSC2
VSS
VCCX
VCC
TEST
TX4
TX3
TX2
TX1
R3
47K
228
C2
1nF
230
216
S1
S2
B1
3.6V
214

FIG. 6B

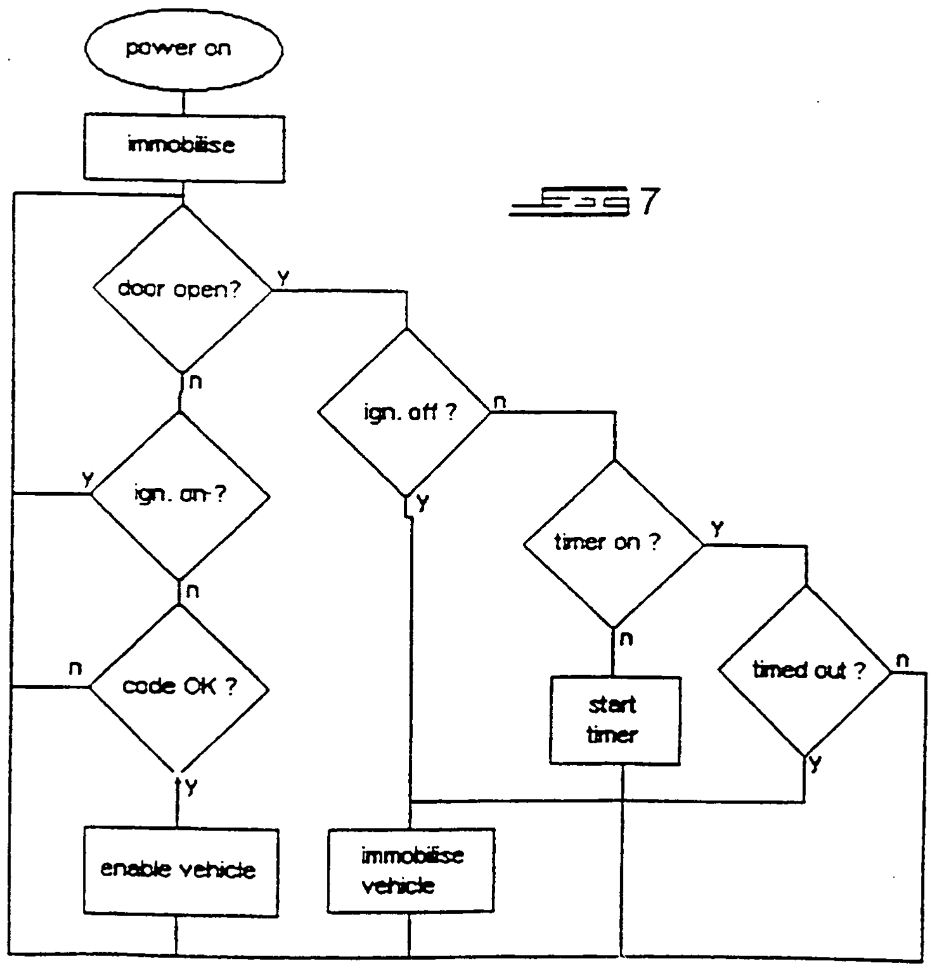

power on
immobilise
door open?
ign. off ?
ign. on ?
timer on ?
code OK ?
start timer
timed out ?
enable vehicle
immobilise vehicle
Y
n

FIG. 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 96/02517

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 B60R25/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 354 102 A (RENAULT) 7 February 1990 see column 2, line 30 - column 3, line 37 ---	1,2,8
Y	EP 0 475 800 A (ADESCO SARL) 18 March 1992 see column 2, line 4-40 ---	1,2, 8-10,17
Y	GB 2 286 702 A (GARDNER ANDREW) 23 August 1995 see abstract ---	1,2, 8-10,17
A	GB 2 270 182 A (PILKINGTON MICRO ELECTRONICS) 2 March 1994 see abstract ---	1
Y	GB 2 253 930 A (GEC FERRANTI DEFENCE SYST) 23 September 1992 see column 2, line 11-22 ---	4,14-16
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1 Date of the actual completion of the international search 30 June 1997	Date of mailing of the international search report 04. 07. 97
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Authorized officer Waldorff, U

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 96/02517

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 276 728 A (PAGLIAROLI KENNETH ET AL) 4 January 1994 see column 4, line 8-45	4,14-16
A	US 5 315 286 A (NOLAN MICHAEL J) 24 May 1994 see column 2, line 23 - column 3, line 2	3,5-7, 11-13,16
A	DE 43 14 064 A (TELEFUNKEN MICROELECTRON) 3 November 1994 see abstract	3
A	WO 81 03002 A (BLAIS AUTO SECURITY CORP) 29 October 1981 see page 3, line 9 - page 5, line 7	8

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 96/02517

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0354102 A	07-02-90	FR 2634706 A	02-02-90
		DE 68912445 D	03-03-94
		DE 68912445 T	26-05-94
		ES 2049836 T	01-05-94
EP 0475800 A	18-03-92	FR 2666059 A	28-02-92
		DE 69101044 D	03-03-94
		DE 69101044 T	04-08-94
		ES 2051093 T	01-06-94
GB 2286702 A	23-08-95	NONE	
GB 2270182 A	02-03-94	AU 670304 B	11-07-96
		AU 4487993 A	21-04-94
		CA 2105011 A	01-03-94
		EP 0586192 A	09-03-94
		JP 7002058 A	06-01-95
GB 2253930 A	23-09-92	NONE	
US 5276728 A	04-01-94	NONE	
US 5315286 A	24-05-94	NONE	
DE 4314064 A	03-11-94	NONE	
WO 8103002 A	29-10-81	AU 7172081 A	10-11-81
		BR 8108572 A	06-04-82
		CA 1163008 A	28-02-84
		EP 0050655 A	05-05-82
		JP 57500602 T	08-04-82